Research and Development Projects Launched in Response to the Dynamic Evolution of Internet Security Threats – A Perspective of a CERT Team

Piotr Kijewski, Mirosław Maj, Krzysztof Silicki
NASK / CERT Polska
Warsaw
POLAND

piotr.kijewski@cert.pl / miroslaw.maj@cert.pl / krzysztof.silicki@nask.pl

ABSTRACT

Wherever they are, CERTs (Computer Emergency Response Teams) as security incident handlers have hands-on experience with the latest attack techniques on the Internet. This is the result of direct contact with their constituency and other CERT teams, which often serve as the first line of support when faced with new threats. The dynamic development of threats remains a never ending challenge not just for them, but the entire security industry. Research and development projects that are launched in response to analyzing threats, often have a problem keeping up and developing adequate tools that can be applied in practice. Nevertheless, creating new platforms that can facilitate detection and improve situation awareness is critical in order to stop these threats.

1.0 INTRODUCTION

The article presents technical issues concerning national and international research and development projects conducted by the CERT Polska team, operating in NASK structures.

We present how these projects support the operational activity of CERT, which determines the requirement for new tools and research – namely for projects having practical application in e.g. threat monitoring, correlation, early warning, malware analysis or effective transfer of information to proper recipients.

A few examples of building synergy between projects being implemented are presented. As an example, a fully operational early warning system ARAKIS, based on monitoring the network in terms of threats that propagate through active means (e.g. network worms, botnets) is being supplemented through new a Honey Spider Network project – focused on *"drive-by-download"* attacks. This is in response to the recent trends in observed attack techniques, as reported by our CERT constituency. Information acquired in such a manner is used in another European project – WOMBAT, a global observatory of threats, confronting locally observed processes with phenomena noticeable in other parts of the globe. Thereby relations between projects are established, new modules and interfaces developed, which bind existing solutions to new ones – creating at the same time an area of research and development projects, which are used in practice in CERT environment and public administration units.

2.0 THE MAIN TECHNICAL PROJECTS OF CERT POLSKA TEAM

2.1 The ARAKIS Project

The ARAKIS system is an early warning system intended to improve situational awareness of what is happening in terms of attacks observed in Polish address space. The system consists of a distributed

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2010	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Research and Development Projects Launched in Response to the Dynamic Evolution of Internet Security Threats A Perspective of a CERT Team	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **NASK / CERT Polska Warsaw POLAND**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADA564697. Information Assurance and Cyber Defence (Assurance de l'information et cyberdefense). RTO-MP-IST-091

14. ABSTRACT
Wherever they are, CERTs (Computer Emergency Response Teams) as security incident handlers have hands-on experience with the latest attack techniques on the Internet. This is the result of direct contact with their constituency and other CERT teams, which often serve as the first line of support when faced with new threats. The dynamic development of threats remains a never ending challenge not just for them, but the entire security industry. Research and development projects that are launched in response to analyzing threats, often have a problem keeping up and developing adequate tools that can be applied in practice. Nevertheless, creating new platforms that can facilitate detection and improve situation awareness is critical in order to stop these threats.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**8**	

network of sensors that run honeypots and collect data from firewalls and antivirus systems. Most of the functionality comes from the honeypots. We focus on two aspects: a) near real-time detection of malicious activity from a subset of IPs that are of interest to us b) discovering new forms of attack on the Internet. In the case of a) we simply maintain lists of IPs that should never be seen connecting to any of the honeypots and generate an alert if such a situation occurs. For b) we do not employ intrusion detection signatures as the main method for identifying attacks. Instead, we monitor differences in content of packets that are seen by the honeypots. We cluster packets that are similar, and attempt to generate signatures that describe them. These signatures are then sent from all sensors (honeypots) to a central repository where they are clustered again. A current set of clusters is maintained. In theory, whenever a new attack appears, it may generate packet content that is sufficiently different from existing ones, thus forming a new cluster. Such new clusters need to be investigated manually to verify if that is indeed the case.

2.2 The HoneySpider Network Project

The HoneySpider Network (HSN) project, a joint effort with GOVCERT.NL and SURFnet is a project initiated in response to the shift in trends in Internet attacks. More and more often, users' computers are compromised through client side applications and their interaction with malicious web servers. The goal of the HoneySpider Network project is to detect malicious web sites that exploit browser flaws and install malware without awareness of the user (so called drive by downloads). The project is one of the first attempts in the CERT community at building a complete framework for the bulk processing of URLs by various types of client honeypots.

The client honeypots can be low or high interaction. The low interaction client honeypots are web crawlers that attempt to emulate browser behavior. As part of our work, we discovered that open source client honeypot solutions do not meet our expectations, especially in terms of stability and detection rates. This forced us to develop our own crawlers. They use various heuristics to determine whether web site content that is being served is suspicious or malicious. For example, we developed our own machine learning algorithm to distinguish and classify JavaScript code, along with our own DOM implementation. We are continuously working on developing new detection methods to better take into account Flash, ActiveX and PDF components. In HSN, once URLs are analyzed by low interaction crawlers, they can be forwarded to high interaction machines, which consist of real operating systems running real browsers with plugins. System calls invoked during visitation of a web site are captured, allowing for the monitoring of file, process and registry changes. These changes are then compared against exclusion lists (lists that specify what changes are good or bad) to identify potential malicious web sites. As the basis of this solution, a heavily modified open source Capture-HPC 2.5.1 solution is used, which fixes numerous bugs in the software to improve stability and allows it to operate using VirtualBox. Through such an approach, it is often possible not just to identify whether a URL was malicious, but also to obtain malware.

2.3 The WOMBAT Project

Both ARAKIS and the HoneySpider Network project are concerned with better detection and collection of data for further analysis. This is where another of the projects we are involved in, WOMBAT, comes in. The Worldwide Observatory of Malicious Behaviour and Attack Threats is an EU FP7 project that aims to create a common framework for the analysis of malicious activity on the Internet with the ultimate goal of performing threats intelligence and providing attack attribution. One of the achievements of the project is the creation of the WOMBAT API (WAPI) that enables the querying of various other systems (such as Virustotal, Anubis, HSN etc) from a shell application. Various datasets can then be compared without knowledge of the underlying database structure. Security specialists can perform detailed investigation of Internet security incidents, piecing together what various systems know about a specific incident – information such as IPs, malware found, URLs involved etc.

2.4 The FISHA Project

Ultimately, one of the goals of all the above systems is to increase awareness of what is going on in the Internet, provide alerting and warning, best practice information to a wider spectrum of users, primarily private citizens and SMEs. However, none of the above mentioned systems have the capability to do so. To this end, we are one of the initiators of the FISHA project – an EU project the aims to create a framework for information sharing and alerting in Europe. It is intended to operate on the basis of existing national and private sector information and alert sharing systems. One of the project main tasks is to design a prototype of a dedicated web portal, addressed to those target groups. Ultimately, it is planned that each EU Member State will have its own, national portal where up-to-date and easy-to-understand information on various IT computer security aspects, collected under EISAS, will be published. In addition to portals, special information and education campaigns are planned to effectively reach those particular communities.

3.0 PROJECTS AND CERT SERVICES INTERACTIONS

3.1 The Evolution of Threats and Their Influence on Selection of Projects

During years of professional activity of CERT Polska it was easy to observe natural evolution of online threats. That has a crucial impact on selection of research and development projects in which CERT Polska is engaged. In table below there is an illustration of main functionalities of particular project implemented in response to group of threats they dealing with. On the other hand Figure 1 illustrates how evolution of threats influenced development and evolution of project (eg. HSN project was launched to response client side threats not covered by ARAKIS project) as well as benefits one project has from other projects (here in terms of possibility of data acquisition).

Table 1: CERT Polska projects characteristics in terms of functionality and threat categories

	Threats	Functionality
ARAKIS	Network scanning Viruses Worms Zero day exploits	Detection of anomalies Watch and warning Data collection Alerting Trend observation
HONEY SPIDER NETWORK (HSN)	Malware Drive-by-download infections Infected websites Client application attacks	 Threat crawling Active malware searching Data collection

WOMBAT	Malicious software On-line threats Underground economy	Global system Data collection Monitoring Threat analysis Identification of threat sources Data sharing
FISHA	Lack of awareness Lack of cooperation Lack of information sharing	Information sharing Alerting Awareness raising Pan European network of web portals

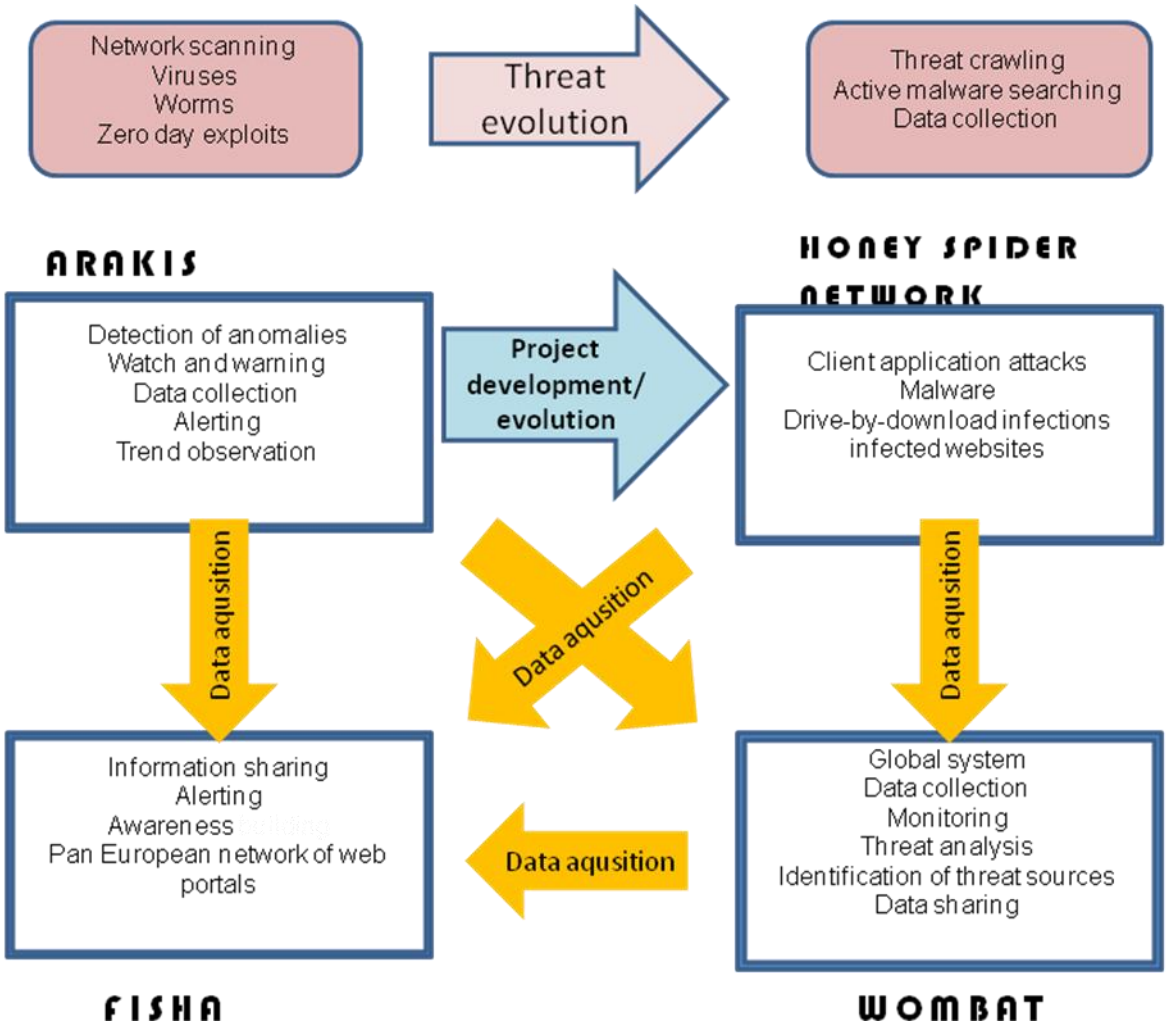

Figure 1: The evolution of threats and their influence on selection of projects

3.2 Relations between Technical Projects and CERT Services

All mentioned projects have a direct influence on CERT services. Especially they improve a quality of existing services but also can cause launching new services for CERT constituency. Very often decision about entering a new project is a consequence of needs identified by CERT staff who provides services.

The table and a schema below show relationship between CERT Polska projects and some services. The list of services is not complete. The entire list has more positions and was developed by experts from CERT Coordination Center at Carnegie Mellon University (http://www.cert.org./csirts/services.html)

Table 2: Relationship between CERT Polska projects and common CERT services

CERT SERVICES / CERT Polska Projects	ARAKIS	HSN	WOMBAT	FISHA
REACTIVE SERVICES				
Alerts and Warnings	x	x		x
Incident Handling	x	x	x	
Artifact Handling	x	x	x	
PROACTIVE SERVICES				
Announcements				x
Technology Watch				x
Security Audits and Assesments	x	x		
Intrusion Detection Services	x	x	x	
Security-Related Information Dissemination	x			x
SECURITY QUALITY MGMT SERVICES				
Risk Analysis		x	x	
Security Consulting				x
Awareness Building				x

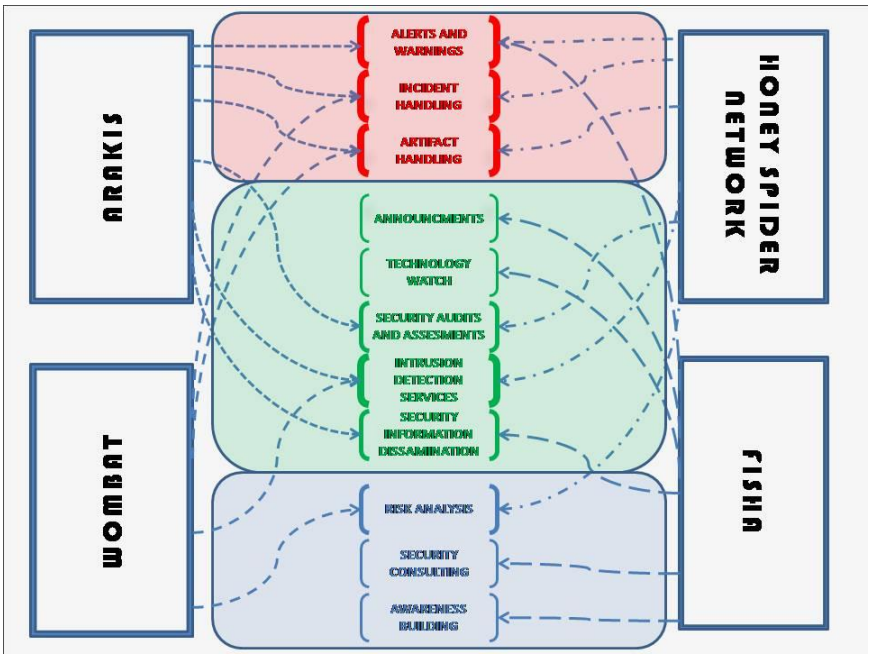

Figure 2: Influence of particular CERT Polska projects on services the team provides